NALS PRACTICAL

PRACTICAL 8: Identify Phishing

Answer: A phishing attack can be identified by carefully analyzing the content, structure, and intent of a digital message such as an email, SMS, or social media notification. Phishing is a type of cybercrime where attackers pretend to be trusted organizations or individuals in order to steal sensitive information like login credentials, banking details, or personal data. The first step in identifying such an attack is to read the message thoroughly and observe the sender's identity. Phishing messages often come from unknown, misspelled, or suspicious email addresses that imitate official domains.

There are several common signs that indicate a phishing attempt. One major indicator is the presence of spelling and grammatical errors, which are rarely found in official communications. Another sign is the use of urgent, threatening, or fear-inducing language such as "act immediately," "account suspended," or "verify now," which pressures the user into taking quick action without thinking. Phishing messages may also contain suspicious or shortened links that redirect users to fake websites designed to look like legitimate ones. These fake websites often ask for usernames, passwords, OTPs, or card details. Additionally, messages offering rewards, lottery winnings, refunds, or prizes that the user never applied for are strong indicators of a scam.

Phishing attacks can also include attachments that claim to be invoices, receipts, or documents. Opening such attachments may install malware or spyware on the user's device. Another red flag is when the message asks for confidential information directly, as genuine organizations do not request sensitive data through emails or messages. The lack of personalization, such as using generic greetings like "Dear User" instead of the recipient's real name, is also a common phishing characteristic.

Based on these suspicious elements, the message can be categorized as a phishing attack or online fraud. To verify the authenticity of the message, users should check the sender's email address carefully, hover over links to inspect the actual URL, and avoid clicking on unknown links or downloading attachments. It is safer to visit the official website directly by

typing the URL in the browser instead of using provided links. Contacting the organization through official customer support channels and using antivirus or email filtering tools further helps in confirming legitimacy. Awareness of these warning signs and verification steps plays a crucial role in protecting individuals from phishing attacks and reducing cybercrime risks.